Technical Bulletin No. 332

ENHANCE SECURITY REQUIREMENTS FOR SYSTEM ACCESS

Issued Date: December 29, 2003
Effective Date: March 31, 2004
Section/Group: ITS Information Security Office
Submitted By: Michael Allred
Approved By: Norm Johnson

The purpose of this bulletin is to clarify the ITS Information Security Office (IISO) position on access to information systems.

Recently passed State and Federal legislation require that increased security measures be implemented to protect personal information transmitted and stored on State of Utah information systems. The recommendations coming from HIPAA and the IRS are considered industry standard "best practice" for security. These recommendations require that personal information about individuals collected by the State be encrypted while being transmitted between, or stored on, systems, as well as encrypted authentication mechanisms.

In the past the State has allowed the use of Telnet and 3270 emulation on port 23 to provide users with terminal access to servers and the mainframe. This information is transmitted clear text (un-encrypted) across the State's network. HIPAA and IRS requirements have changed and this information now needs to be transmitted over an encrypted session. In order to accommodate this workstation-to-server communication, ITS has purchased licenses for a 3270 emulator called BlueZone. The ITS Information Security Office also recommends the use of secure shell (SSH) products to replace standard Telnet to UNIX, Linux, and Windows NT boxes.

Starting on March 31, 2004, ITS will block inbound traffic from the Internet to port 23 (Telnet, 3270). Future plans include blocking port 23 access to the mainframe and all UNIX/Linux servers managed or hosted by ITS. This will include those on the State WAN as well. A timeframe has not been established at this time. This change will happen prior to the April 2005 HIPAA deadline.

State agencies should begin today to identify any affected systems or processes and work with the IISO to find solutions to achieve this objective.

ITS is also working on solutions for secure file transfer (SFTP) between systems and will be providing additional information as it become available. As this can be application specific, ITS depends on agency requirements in order to recommend a proper solution.

Recommend Solutions:

- Mainframe 3270 Emulation—BlueZone or other SSL enabled product.
- Telnet—Secure shell products, including PuTTY or SSH.
- External access can be achieved using an ITS provided VPN solution.

Please contact the ITS Customer Service for Questions on BlueZone and this change.